IN THE SPECIFICATION

Page 5, line 15 through page 6, line 15 REPLACE as follows:

C 1 In Fig. 1 a broadband, shared link, multi-user network 10, such as a cable, satellite, radio, LAN/Wan includes a network 11 coupled a plurality of customers 12^1, 12^2...12^n and an Internet Service Provider (ISP) 14 associated with the network 10. For simplicity, the broadband network 10 will be described in terms of a cable network 11 in which the customers 12^1...12^n include cable modems 16^1, 16^2.... 16n which link the customers through a broadband cable 18 to a cable affiliated ISP server 20. Typically, the cable modems use an Ethernet protocol for the computers 13^1, 13^2 and 13^n. The modems look like any LAN network to the computer. The computers use a frequency shift to put an Internet protocol into a given channel assignment on the cable 18. Typically, the modems 16', 16^1 share the last mile of the cable to the server 20. As a result, the server cannot send responses back to the cable or broadband customers based on an individual line or port connection point as in the case of a dial-in modem connection to the Internet. In the latter case, an ISP attaches the user to an authentication server, typically a Remote Authentication Dial in User Services (RADIUS) server which is a software-based security authentication protocol developed by the ~~International~~ Internet Engineering Task ~~force~~ Force (IETF) RADIUS Working Group and available from a number of suppliers including Microsoft, Redmond, Washington. RADIUS provides access to all Internet services using one username and password. If the authentication is correct, the customer is assigned a temporary IP address from the ISP's pool of available addresses using a protocol called Dynamic Host ~~connection~~ Configuration Protocol (DHCP). DHCP provides a mechanism through which computers using ~~Transaction~~ Transmission Control Protocol/Internet Protocol (TCP/IP) can obtain protocol configuration parameters automatically through the network. The most important

C1 configuration parameter is an IP address carried by DHCP and assigned to a computer from a pool of IP addressees managed by DHCP. DHCP is an open standard, developed by the Dynamic Host Configuration working group (DHC WG) of the Internet Engineering Task force (IETF).

Page 8, line 8, REPLACE as follows:

C2 Currently, there is no way to enable a group of cable users to choose an ISP not affiliated with the cable company. The customer may send a connection request to their ISP and to the related authentication server, but since the network authentication server is not yet assigned the customer's IP address to them, there is no way for the server return message to be routed back to the customer.

Page 9, line 3 through page 10, line 9, REPLACE as follows:

C3 Returning to Fig. 2, prior to sign on the customer contacts an ISP(s) for Internet service and is provided with a user ID, password and logon script. The customer information is recorded in a database(s) 40, 41,43, as the case maybe. Upon sign on the customer authentication function is accomplished in a cooperative manner between different servers, the BMPS and the selected ISP server. The BMPS processes the initial customer DHCP logon request. The request may or may not have a server or client IP address identified per the standard Internet DHCP process. The underlying protocol can be whatever protocol is supported by the cable modem. As part of the logon message, the MAC address is attached to identify the origination point of the message. This MAC address is placed in the client hardware address field, Fig. 3a 32-7, of the DHCP package. The BMPS checks the modem MAC address against the modem management system to verify the customer is legitimate and then obtains and records the customer profile for management and billing purpose in the database 23'. The server 21 sends the logon request to

the selected ISP on behalf of the customer using the DHCP message 30 and the extended DHCP message 39 (See Figs. 3A and 3B) including the customer or end user ID and password or another unique identifier. The ISP server checks the ID and password in the associated database 40, 41, 42, as the case maybe, for authentication and if legitimate proceeds as normal returning an IP address assignment to the source address i.e., the server 22 using the DHCP message formats 30 and 39. The server 22 updates the database 23 and routing table in router 21' so as to allow future customer messages with the authenticated address to traverse the links authorized to the selected ISP. The customer updates his address mechanism with a valid IP address for IP usage. Future IP packets flow from the customer to the router 21' then to the selected ISP which forwards the message to the message destination. Return packets from the message receiver reverse the route to the customer. The server 22 can remain in the serial path if desired to continue to check on the validity of the packet and count the packets for billing purposes traversing the links or the server 22 can be removed from the link allowing the packets to flow directly to the router, as described. When the Internet session is over, the selected ISP sends the BMPS 22 a sign out message for the assigned address that was used. Thereafter, the BMPS 22 will remove that source address of the valid source or destination address in the router table.